

# MP-IDSA *Commentary*

## The First AI War: The Dilemma of Military Autonomy

*Meghna Pradhan*

March 23, 2026

### **S***ummary*

The war in West Asia has seen an unprecedented use of Artificial Intelligence and autonomous systems like drones in the military kill chain.

The eruption of high-intensity hostilities in the Persian Gulf in late February and early March 2026, initiated jointly by the US and Israel and dubbed ‘Operation Epic Fury’ or ‘Operation Roaring Lion’ by respective nations, represents a watershed moment in the history of armed conflict. Aimed at conducting ‘decapitation strikes’<sup>1</sup> on Iran’s nuclear infrastructure, command-and-control centres, and senior leadership, the conflict has seen a rapid escalation in kinetic and cyber domains. More importantly, the event served as kindling for what is being called the first full-scale ‘AI war’.<sup>2</sup>

The designation is not purely rhetorical. There has been unprecedented use of AI-driven assets as Decision Support Systems (DSS), not merely as secondary analytical tools but as active enablers of kill chains. Typically, the process of gathering intelligence, identifying targets, conducting simulations and damage assessments, performing predictive analyses, assigning weapons, and executing missions took weeks, if not months, of human deliberation. However, the current war has seen attacks executed faster than ‘the speed of thought’, exemplified by the US conducting almost 900 strikes on Iranian targets in the first 12 hours alone and over 5,500 strikes in the first 10 days.<sup>3</sup>

To achieve such unprecedented scale, precision, and velocity in attacks, the United States Central Command (CENTCOM) leveraged advanced AI tools, such as Palantir’s MAVEN Smart System (MSS), which was integrated with Anthropic’s Claude LLM. These assets were using troves of unstructured, classified data from satellites, surveillance, and other intelligence, helping to provide pattern development, real-time targeting, and target prioritisation.<sup>4</sup> For instance, the precision strikes that led to assassination of Iran’s supreme leader, Ayatollah Ali Khamenei<sup>5</sup> and marked beginning of the war, was done by methodical use of AI and cyber espionage – the cameras in Tehran were hacked over the years, recording and feeding massive amounts of presumably mundane data (parking, personnel, traffic light timings, etc.) to Israel. This data, in turn, was used to map patterns and layouts, and ultimately to run predictive analyses for simultaneous and precise strikes.

The US has also developed and deployed Low-cost Unmanned Combat Attack System (LUCAS), a ‘Kamikaze’ drone system, as a cost-efficient high-volume defence asset

---

<sup>1</sup> Graham Scarbro, “[Iran-Israel Conflict: A Quicklook Analysis of Operation Rising Lion](#)”, *US Naval Institute*, June 2025.

<sup>2</sup> Larisa Brown, “[The first AI war: US and Israel use Iran to test autonomous tech](#)”, *The Times*, 10 March 2026.

<sup>3</sup> “[US says 5,500 targets hit in Iran as operation continues](#)”, *Middle East Monitor*, 11 March 2026.

<sup>4</sup> Tara Copp; Elizabeth Dwoskin; Duncan, “[Anthropic’s AI tool Claude central to U.S. campaign in Iran, amid a bitter feud](#)”, *The Washington Post*, 4 March 2026.

<sup>5</sup> Mehul Srivastava, James Shotter, Neri Zilber, Steff Chávez, “[Inside the plan to kill Ali Khamenei](#)”, *Financial Times*, 2 March 2026.

against Iran. At a production cost of USD 35,000, these drones offer a lower-cost alternative compared to US Tomahawk Land Attack Missiles, which cost upward of USD 2.4 million per shot.<sup>6</sup> Interestingly, LUCAS drones were reverse-engineered from Iran’s HESA Shahed-136 drones, which have gained notoriety in the Ukraine-Russian war. These drones are equipped with artificial intelligence that enables them to perform autonomous and swarm manoeuvres. The integration of LUCAS marks significant departures from the conventional understanding of asymmetric warfare. One, there is a realisation in the US that sophistication is not the only benchmark of military capability, and that cost and mass can be decisive factors. Secondly, the earlier logic of the flow of technology from more advanced to less advanced states no longer necessarily holds.<sup>7</sup>

Iran has similarly leveraged drone saturation and cyber warfare against the US and Israel. Iranian drone strikes have allegedly been responsible for the deaths of six US military personnel in Kuwait.<sup>8</sup> These attacks are also being used for targeting data infrastructures; of the six data facilities that the US company Amazon has in the UAE, three were allegedly struck by Iranian drones.<sup>9</sup> Iranian hacker group Handala has also reportedly targeted US and Israel-based entities, including Israel’s Air Force personnel, Israel Meteorological Systems, US-based medical technology firm Stryker and Hebrew University.<sup>10</sup> There are indications that the diminished timeline for their scale of attacks may be due to AI-assisted reconnaissance.<sup>11</sup> Furthermore, allegations have emerged that Iran has been actively leveraging AI for disinformation campaigns in the media.<sup>12</sup> Notably, Iran is currently facing an internet blackout, indicating that these cyberattacks are occurring through proxies distributed outside the country, indicating a significant degree of diffusion in its asymmetric cyber and autonomous capabilities.

The advantages of AI and drones, such as decision compression and low-cost saturation, have also proven to come with high human costs. The hyper-condensed decision-making cycle leaves little room for the human operator to cross-verify.

---

<sup>6</sup> Zita Ballinger Fletcher, “[America Reverse-Engineered Iran’s Most Decisive Weapon—Then Launched It Against Its Creators](#)”, *Popular Mechanics*, 13 March 2026.

<sup>7</sup> Steve Feldstein, Dara Massicot, “[What We Know About Drone Use in the Iran War](#)”, *Carnegie Endowment for International Peace*, 2 March 2026.

<sup>8</sup> Abené Clayton, “[Pentagon releases names of final two soldiers of six killed in Kuwait](#)”, *The Guardian*, 5 March 2026.

<sup>9</sup> Julian Fell, Ashley Kyd, Jarrod Fankhauser, Matt Liddy, “[AI is helping choose targets in Iran war — now it’s a target too](#)”, *ABC News*, 15 March 2026.

<sup>10</sup> Andy Greenberg, Matt Burgess, Lily Hay Newman, “[How ‘Handala’ Became the Face of Iran’s Hacker Counterattacks](#)”, *The Wired*, 12 March 2026; Aakash Sharma, Khooshi Sonkar, “[Pledged to Iran’s new leader, hackers wage digital war on US and Israel](#)”, *India Today*, 16 March 2026.

<sup>11</sup> Ibrahim Saify, “[AI, the Iran-US Conflict, and the Threat to US Critical Infrastructure](#)”, *CloudSEK*, 6 March 2026.

<sup>12</sup> Kenrick Cai, “[Trump accuses Iran of using AI to spread disinformation](#)”, *Reuters*, 16 March 2026.

Reliance on AI-accelerated decision-making, which is often plagued by outdated data and a lack of rigorous human verification, has direct implications for human casualties. The March 2026 war has illustrated these costs, as drone attacks from both sides of the war have hit civilian infrastructure and population directly, or have caused damage due to ensuing debris, shrapnel and fires.

For instance, on 28 February 2026, a Tomahawk cruise missile reportedly hit near Shajareh Tayyebbeh Girls’ Primary School in Minab, causing over 170 casualties, mostly consisting of children under the age of 12.<sup>13</sup> The school was located near an Islamic Revolutionary Guard Corps (IRGC) facility. It was likely not recognised by AI-driven target identification systems as a separate building because of outdated intel dating back to 2016.<sup>14</sup> Similarly, in a bid against military infrastructure in Tehran, a residential complex in Resalat Square, Tehran, had also become a site for airstrikes, leading to over 40 civilian casualties.<sup>15</sup>

Multiple reports suggest that the US and Israeli warheads have been hitting civilian sites such as schools, hospitals<sup>16</sup>, as well as protected structures and historic landmarks such as Golestan Palace in Tehran, and Chehel Sotoun Palace in Isfahan. Iran has, in retaliation, initiated strikes in the UAE, leading to fires near the US Consulate in Dubai and impacting civilian areas like Burj Al Arab, Dubai Airport and Jebel Ali seaport.<sup>17</sup> In Israel, Iranian drone-based retaliation has reportedly caused over 18 deaths and 3100 injuries among civilian and military personnel alike.<sup>18</sup>

These caveats have also extended to the battlefield. For instance, the increased use of drone swarming tactics may overwhelm airspace and overload signature interception for defence systems. The downing of three U.S. F-15E Strike Eagles in friendly fire by Kuwaiti F/A-18 on March 1, 2026, exemplifies this perfectly. As an active target of Iran’s missile and drone attacks, Kuwait’s air defence was primed to attack. It mistakenly targeted US fighter jets during a high-tension, active combat situation.<sup>19</sup>

---

<sup>13</sup> Malachy Browne, John Ismay, [“U.S. Tomahawk Hit Naval Base Beside Iranian School, Video Shows”](#), *The New York Times*, 8 March 2026.

<sup>14</sup> Elizabeth Melimopoulos, [“Who bombed the Iranian girls’ school, killing more than 170? What we know”](#), *Al Jazeera*, 12 March 2026; Al Jazeera Staff, [“Al Jazeera investigation: Iran girls’ school targeting likely ‘deliberate’”](#), *Al Jazeera*, 3 March 2026.

<sup>15</sup> Mahmoud Aslan, [“Rescue Efforts in Tehran After a Triple Strike Hit Apartment Buildings, Killing 40”](#), *Drop Site*, 12 March 2026.

<sup>16</sup> Paul Brown, Shayan Sardarizadeh, Matt Murphy, [“Iranian schools, hospital and landmarks among civilian sites hit during US-Israeli strikes”](#), *BBC*, 6 March 2026.

<sup>17</sup> AFP, [“Iran attacks rock Dubai's Palm, Burj Al Arab, airport”](#), *The Hindu*, 2 March 2026.

<sup>18</sup> Moiz Mustafa, [“Breaking Down the Israel-Iran Conflict: What We Know So Far - Day 16”](#), *Daily Mirror*, 16 March 2026.

<sup>19</sup> ETOonline, [“US-made Kuwaiti jet mistakenly shot down three US F-15s, probe finds: WSJ”](#), *The Economic Times*, 4 March 2026.

These incidents have therefore underscored an important aspect of AI-driven warfare: while AI may guarantee decision compression, it does not necessarily prevent catastrophic human costs. The technology continues to develop and remains vulnerable to ‘algorithmic brittleness’<sup>20</sup>, thereby frequently leading to violations of International Humanitarian Law. The very foundational promise of AI in warfare, of reduction in collateral damages due to precision, elimination of human error, and making combat operations safer for civilians and military personnel alike, seems to have remained considerably unfulfilled.

Additionally, the unprecedented speed and scale afforded by AI seem to have accelerated speed for resultant casualties; deaths that might have previously occurred over the course of a month can now happen in a matter of hours or days. Taken together, it is clear that integrating highly sophisticated tools and greater machine autonomy, without appropriate guardrails and meaningful human oversight, may likely worsen the overall human cost of war rather than reduce it.

Notably, several critical diplomatic initiatives were unfolding concurrently with the war in West Asia, grappling with these exact dilemmas. In February, weeks before the conflict broke out, global leaders had convened at A Coruña, Spain, for the Responsible Artificial Intelligence in the Military Domain (REAIM) Summit. Similarly, just a couple of days after Operation Epic Fury/Roaring Lion was initiated, the UN Convention on Certain Conventional Weapons (CCW) held its Group of Governmental Experts (GGE) session on autonomous weapons in Geneva.

There is a stark sense of irony to the timing of these events: as diplomats debate the nuances of human-machine interaction, legal reviews, and definitions of autonomy, major powers are actively leveraging these systems unchecked on the battlefield. Furthermore, even as the urgency to regulate military AI peaks, the number of signatures on instruments that actively advocate for responsible military AI has declined. The ‘Pathways to AI’, formulated after REAIM 2026 in Spain, received only 35 signatures out of the over 80 countries attending, with total abstention by major powers (including the primary countries engaged in the current conflict<sup>21</sup>). Dutch defence minister Ruben Brekelmans mentioned how governments face a ‘prisoner’s dilemma’, where they are caught between setting limits in military AI and avoiding restrictions that, amidst an escalating arms race, their rivals may ignore.<sup>22</sup>

---

<sup>20</sup> This refers to a condition where an algorithm may not be able to generalize or adapt to conditions outside a narrow set of assumptions. In such a situation, while AI may perform well under certain conditions, especially during training, it may not perform optimally, or even fail, when exposed to new, unexpected, or slightly modified inputs.

<sup>21</sup> Oumaima Moho Amer, “[Morocco Joins 34 Countries in Endorsing ‘Pathways to Action’ Pact Towards Safe Governance of Military AI](#)”, *Morocco World News*, 6 February 2026.

<sup>22</sup> ETEnterpriseAI Desk, “[AI weapons regulation: Nations divided as US, China skip global pledge](#)”, *ET Enterprise AI*, 6 February 2026.

The ‘first AI war’, therefore, has created a significant paradox: on one hand, the ongoing (and unchecked) expansion and use of military AI has severely undermined global diplomatic efforts. It calls into question the efficacy of processes that discuss theoretical constraints and debate semantics, which state actors may readily abandon in favour of overwhelming tactical advantages. On the other hand, the civilian casualties and socio-cultural losses wrought by the Iran war underscore the very necessity of these discussions and debates. Even as forums like UNCCW and REAIM struggle to keep pace with the integration of AI into military operations, forging consensus on robust guardrails that balance the expansion of autonomous capabilities with clear human accountability has become increasingly urgent.

The March 2026 conflict in West Asia, therefore, has fundamentally altered perceptions and calculations about modern warfare. As the proclaimed first full-scale ‘AI war’, it has served as a proving ground for artificial intelligence and autonomous systems in a military context. We are witnessing, in real time, the capabilities of algorithms to be a decisive factor in military engagement by accelerating military operations beyond the capabilities of human cognition. Yet, when seen in the context of the friendly fire incidents and civilian casualties, the delegation of decisions regarding military engagement and lethality to machines also comes with damning costs and critical accountability gaps.

There is thus a need to strike a balance between the necessity of AI and autonomous systems for decision speed and the need for guardrails to prevent human cost and uphold IHL. In the face of real-time geometric growth and proliferation in military AI, the international community faces a challenge of creating frameworks that ensure ethical and legal compliance and meaningful human control over these systems, before human oversight becomes obsolete.

## About the Author



**Ms. Meghna Pradhan** is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

**Manohar Parrikar Institute for Defence Studies and Analyses** is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

*Disclaimer:* Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

© Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) 2026